CYBERSECURITY GUIDANCE: CHINESE-MANUFACTURED UAS

OVERVIEW

Chinese-manufactured unmanned aircraft systems (UAS), more commonly referred to as drones, continue to pose a significant risk to critical infrastructure and U.S. national security. While any UAS could have vulnerabilities that enable data theft or facilitate network compromises, the People's Republic of China (PRC) has enacted laws that provide the government with expanded legal grounds for accessing and controlling data held by firms in China. The use of Chinese-manufactured UAS requires careful consideration and potential mitigation to reduce risk to networks and sensitive information. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) encourage U.S. critical infrastructure owners and operators to procure UAS that follow secure-by-design principles, including those manufactured by U.S. companies. CISA and FBI further recommend following principles and implementing cybersecurity recommendations listed in this guidance to any organization procuring and operating UAS.

THREAT

The White House's 2023 National Cybersecurity Strategy and the Annual Threat Assessment from the Office of the Director of National Intelligence both recognize the PRC as the most advanced, active, and persistent cyber threat to the United States. Their analysis describes how the PRC expanded cyber operations to challenge the global order and U.S. interests. Central to this strategy is the acquisition and collection of data - which the PRC views as a strategic resource and growing arena of geopolitical competition.[1]

Since 2015, the PRC has passed or updated comprehensive national security, cybersecurity, and data privacy laws and regulations, expanding their oversight of domestic and foreign companies operating within China.[2] One of these laws, the PRC's 2017 National Intelligence Law, compels Chinese companies to cooperate with state intelligence services, including providing access to data collected within China and around the world. This includes prominent Chinese-owned UAS manufacturers that the Department of Defense has identified as "Chinese military companies" operating within the United States.[3] The 2021 Data Security Law expands the PRC's access to and control of companies and data within China and imposes strict penalties on China-based businesses for non-compliance.[4] The data collected by such companies is essential to the PRC's Military-Civil Fusion strategy, which seeks to gain a strategic advantage over the United States by facilitating access to advanced technologies and expertise.[5] The 2021 Cyber Vulnerability Reporting Law requires Chinese-based companies to disclose cyber vulnerabilities found in their systems or software to PRC authorities prior to any public disclosure or sharing overseas. This may provide PRC authorities the opportunity to exploit system flaws before cyber vulnerabilities are publicly known.[6]

The use of Chinese-manufactured UAS in critical infrastructure operations risks exposing sensitive information to PRC authorities, jeopardizing U.S. national security, economic security, and public health and safety.

VULNERABILITIES

UAS are information and communications technology (ICT) devices capable of receiving and transmitting data.[7] Each point of connection is a potential target that could be exploited to compromise sensitive information.[8] Avenues of potential compromise include:

Data Transfer and Collection: UAS devices controlled by smartphones and other internet-connected devices provide a path for UAS data egress and storage, allowing for intelligence gathering on U.S. critical infrastructure.

Patching and Firmware Updates: While ensuring that network-connected devices are up to date with the latest patches and firmware is critical for the secure operation of any ICT device, updates controlled by Chinese entities could introduce unknown data collection and transmission capabilities without the user's awareness. That data might be accessed by the PRC through legal authorities.

Broader Surface for Data Collection: As UAS and their peripheral devices such as docking stations are incorporated into a network, the potential for data collection and transmission of a broader type—for example, sensitive imagery, surveying data, facility layouts—increases. This new type of data collection can allow foreign adversaries like the PRC access to previously inaccessible intelligence.

CONSEQUENCE

The PRC's collection of sensitive information and potential network access obtained from Chinese-manufactured UAS may result in significant consequences to critical infrastructure security and resilience. Acquisition of such data or network access has the potential to advance the PRC's strategic objectives and negatively affect U.S. economic and national security by:

- Exposing intellectual property to Chinese companies and jeopardizing an organization's competitive advantage.
- Providing enhanced details of critical infrastructure operations and vulnerabilities increasing the PRC's capability to disrupt critical services.
- Compromising cybersecurity and physical security controls leading to potential physical effects such as theft or sabotage of critical assets.
- Exposing network access details that enhance the PRC's capability to conduct cyber-attacks on critical infrastructure.

MITIGATION

Public and private sector organizations using UAS to collect sensitive or national security information are encouraged to procure, or transition to, secure-by-design systems. This recommendation is emphasized for the federal government in Executive Order 13981 – Protecting the United States from Certain UAS where departments and agencies are required to have a plan that addresses risk from UAS manufactured by a foreign adversary.[9] Organizations can consult the Department of Defense's Blue UAS Cleared List to identify UAS compliant with federal cybersecurity policies.[10]

Organizations procuring or operating UAS are encouraged to adopt the proven security recommendations such as those provided on the next page to further enhance their cybersecurity posture.

UAS CYBERSECURITY RECOMMENDATIONS:

PLAN/DESIGN

Ensure secure, organization-wide development of the goals, policies, and procedures for the UAS program.

- Incorporate UAS and its components into an organizational cybersecurity framework for Internet of Things (IoT) devices, subjecting them to the same level of protection and monitoring as other organizational ICT devices.[11]
- Isolate, air gap, or segment networks to prevent any potential malware or breach from spreading to the enterprise network. Examples of this include setting up separate networks, virtual local area networks (VLANs), or virtual private networks (VPNs).[12] This minimizes the organizational impact from potential cyberattacks.
- Implement a Zero Trust (ZT) framework for the UAS fleet.[13] ZT architecture ensures all network access and transactions are continuously verified and authenticated, minimizing unauthorized access and shrinking the overall attack surface.
- Implement phishing-resistant multifactor authentication methods to secure organizational accounts and data.[14]
- Consider integrating cybersecurity and physical security functions across the organization to achieve a unified approach to risk management.[15]

PROCURE

Identify and select the UAS platforms that best meet the operational and security requirements of the organization.

- Procure UAS that follows secure-by-design principles to proactively address vulnerabilities and emerging threats.[16]
- Understand where UAS are manufactured and to what laws the manufacturer is subject to clarify security standards and assess supply chain risk.
- Review the privacy policy for the chosen UAS, including how and where data will be stored and shared. This is essential for the maintenance of data privacy and security.
- Implement a Supply Chain Risk Management (SCRM) Program for ICT devices to ensure the integrity, security, and reliability of the UAS lifecycle.[17]
- Ensure critical UAS information and communication components undergo a software bill of materials (SBOM) and hardware bill of materials (HBOM) review and consider implementation of long-term SBOM and HBOM management.[18, 19] This minimizes inherent supply chain risks and promotes the resilience of the UAS ecosystem.

MAINTAIN

Perform regular updates, analysis, and training in accordance with the organization's plans and procedures.

- Manage the UAS program in accordance with an information technology (IT) asset framework to ensure proper tracking, monitoring, control, compliance, security controls, and risk management.[20]
- Implement a vulnerability management program to identify, prioritize, acquire, verify, and install firmware patches and updates. This program addresses emerging vulnerabilities and ensures timely application of necessary security fixes.[21]
- Implement a configuration and change management program to maintain adequate security measures and operational capabilities.[22]
- Ensure firmware patches and updates are obtained exclusively from the UAS manufacturer or trusted third-party to minimize the risk of system compromise.
- Consider the use of a sandbox or standalone terminal for the download and security verification of firmware patches and updates. This provides an isolated environment to verify the file integrity and mitigate any concerns before introducing it to the UAS.[23]
- Perform periodic log analysis and compliance checks to determine if any anomalies exist, allowing for timely identification of unauthorized access attempts.
- Implement an information technology security education and training awareness schedule focused on current threats and best practices. An effective training program allows UAS operators to identify and mitigate risks and respond effectively to emerging cybersecurity threats.[24]

OPERATE

Ensure proper operational and security policies are followed during operational usage.

- Verify current software and firmware versions are installed prior to operational use to minimize emerging threats and vulnerabilities.
- Maintain robust data-at-rest and data-in-transit procedures for encryption and storage to ensure the confidentiality and integrity of data collected via UAS.[25]
- Delete collected data from the UAS to include imagery, Global Positioning System (GPS) history, and flight telemetry data after data has been transferred and stored.
- Remove and secure portable storage such as secure digital (SD) cards from the UAS prior to storage to prevent unauthorized access.
- Maintain a secure connection with the drone during operations by using a virtual private network (VPN) or other encryption method to protect the confidentiality and integrity of communication pathways.
- Do not broadcast or live stream to the internet to prevent the unauthorized acquisition of real-time sensitive data.

RESOURCES

For additional information, please see the following resources:

Unmanned Aircraft Systems: cisa.gov/topics/physical-security/unmanned-aircraft-systems

Secure Your Drone: Privacy and Data Protection Guidance: cisa.gov/resources-tools/resources/secure-your-drone-privacy-and-data-protection-guidance

Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems (UASs): cisa.gov/resources-tools/resources/cybersecurity-best-practices-operating-commercial-unmanned-aircraft

NIST IT Asset Management: csrc.nist.gov/publications/detail/sp/1800-5/final

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

CISA Vulnerability Scanning: cisa.gov/resources-tools/services/cisa-vulnerability-scanning

Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171: csrc.nist.gov/publications/detail/sp/800-172/final

Zero Trust Architecture: csrc.nist.gov/publications/detail/sp/800-207/final

China Cyber Threat Overview and Advisories: cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china

Homeland Security Information Network (HSIN): dhs.gov/homeland-security-information-network-hsin

Domestic Security Alliance Council (DSAC): dsac.gov/

Defense Innovation Unit (DIU): diu.mil/blue-uas-cleared-list

ENDNOTES

1 Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, February 2023, https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf; The White House, National Cybersecurity Strategy, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

2 U.S. National Counterintelligence and Security Center, Safeguarding our Future: U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies, 30 June 2023, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf

3 U.S. Department of Defense, DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021, October 2022, https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/.

4 U.S. National Counterintelligence and Security Center, Safeguarding our Future: U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies, 30 June 2023, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf

5 U.S. Department of State, "Military Civil Fusion and the People's Republic of China," accessed August 16, 2023, https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

6 U.S. National Counterintelligence and Security Center, Safeguarding our Future: U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies, 30 June 2023, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf

7 National Institute of Standards and Technology (NIST), Computer Security Resource Center, "Information and communications technology (ICT)," accessed July 20, 2023, https://csrc.nist.gov/glossary/term/information_and_communications_technology.

8 CISA, Cybersecurity and Physical Security Convergence Action Guide, December 2021, https://cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide.

9 Federal Register, "Protecting the United States from Certain Unmanned Aircraft Systems," January 2021, https://www.federalregister.gov/documents/2021/01/22/2021-01646/protecting-the-united-states-from-certain-unmanned-aircraft-systems.

10 Defense Innovation Unit, "Blue UAS Cleared List," accessed July 20, 2023, https://www.diu.mil/blue-uas-cleared-list.

11 NIST, "Cybersecurity IOT Program," accessed July 20, 2023, https://nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

12 NIST, "SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171," February 2021, https://csrc.nist.gov/pubs/sp/800/172/final.

13 NIST, "SP 800-207, Zero Trust Architecture," August 2020, https://csrc.nist.gov/pubs/sp/800/207/final.

14 CISA, "More than a password," accessed July 20, 2023, https://cisa.gov/MFA.

15 CISA, Cybersecurity and Physical Security Convergence Action Guide, December 2021, https://cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide.

16 CISA, "Secure-by-Design, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software," accessed October 25, 2023 https://cisa.gov/resources-tools/resources/secure-by-design.

17 NIST, "Cybersecurity Supply Chain Risk Management," updated May 2022, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

18 CISA, "Software Bill of Materials (SBOM)," accessed July 20, 2023, https://cisa.gov/sbom.

19 CISA, "Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management," accessed November 1, 2023, https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management.

20 NIST, "SP 1800-5, IT Asset Management," September 2018, https://csrc.nist.gov/pubs/sp/1800/5/final.

21 CISA, CRR Resource Guide: Vulnerability Management Volume 4, 2016, https://cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf.

22 NIST, "SP 800-128, Guide for Security-Focused Config. Management of Info Systems," updated October 2019, https://csrc.nist.gov/pubs/sp/800/128/upd1/final; International Organization for Standardization (ISO), "ISO 10007:2017 – Quality Management – Guidelines for configuration management," 2017, https://www.iso.org/standard/70400.html.

23 NIST, Computer Security Resource Center, "Sandbox," accessed July 20, 2023, https://csrc.nist.gov/glossary/term/sandbox.

24 NIST, "SP 800-50, Building an Information Technology Security Awareness and Training Program," October 2003, https://csrc.nist.gov/pubs/sp/800/50/final.

25 NIST, "SP 800-53 Rev.5, Security and Privacy Controls for Information Systems and Organizations," updated December 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.